# Internet et le respect de la vie privée

Boulanger, Marie-Helene; de Terwangne , Cécile

*Published in:*
Internet face au droit

*Publication date:*
1997

*Document Version*
le PDF de l'éditeur

## I. Risques et enjeux

Le réseau Internet permet de diffuser et d'échanger massivement des informations. La présente contribution s'attache à examiner une catégorie particulière de celles-ci, à savoir les données à caractère personnel, c'est-à-dire celles qui peuvent être rattachées à des personnes physiques identifiées ou identifiables.

L'utilisation de ce type de données dans un espace comme Internet constitue une menace pour les libertés et droits fondamentaux des individus, notamment leur vie privée. La notion de vie privée ne doit pas ici être entendue au sens traditionnel, classique : « la vie cachée, tranquille, choisie ». Il s'agit plutôt de la maîtrise par l'individu de l'information qui circule à son propos, de la maîtrise de son image informationnelle.

Dans ce contexte, il paraît utile de retracer sommairement les possibilités offertes par Internet en la matière, pour identifier les risques et enjeux suscités par ce nouveau phénomène, avant d'envisager les réponses qui peuvent y être apportées, en particulier par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[469].

Tout d'abord, certains serveurs Internet constituent un moyen particulièrement fructueux de rassembler quantité de données personnelles : listes d'étudiants et annuaires de chercheurs édités par les universités[470], données issues de la commercialisation de l'annuaire électronique[471]...

En outre, l'utilisateur d'un serveur Internet fournit lui-même, de manière consciente ou inconsciente, de nombreuses données le concernant. Bien souvent, il communique des données de manière tout à fait volontaire, même s'il n'en mesure pas nécessairement toutes les implications. Ainsi, la personne à la recherche d'un emploi peut être tentée d'utiliser le réseau pour y diffuser son curriculum vitae afin de lui donner un maximum de publicité.

Nombre de services ne peuvent se concevoir en l'absence de données personnelles. La commande de biens auprès d'une firme de vente par

---

469 *J. O. C. E.*, 23 novembre 1995, n° L 281/31.

470 V. A. Mole, « Deux avis de la CNIL relatifs à la diffusion de données nominatives sur Internet : une application anticipée de la directive communautaire », *Droit de l'informatique et des télécoms*, 1996, n° 2, pp. 62-64.

471 Ainsi, en Belgique, une société a développé un site reprenant les données issues de la commercialisation, par Belgacom, de l'annuaire électronique. Ce site permet de retrouver sur base de l'identité d'un individu son numéro de téléphone, son adresse, voire sa profession. Il est vrai que l'interrogation se fait sur une base individuelle et qu'étant donné le risque élevé d'homonymie, une information complémentaire (prénom, domicile) s'avère souvent nécessaire pour retrouver les données relatives à un individu déterminé.

correspondance implique la communication d'informations, ne fût-ce que pour que le produit parvienne à bon port et pour en régler le paiement.

On peut également relever le fait que certains serveurs conditionnent l'accès à leurs services à la transmission de renseignements personnels.

Par ailleurs, la collecte de données personnelles est parfois réalisée de manière nettement moins explicite pour l'utilisateur. L'accès à un site peut, par exemple, être soumis à la communication de l'adresse électronique de celui qui le consulte. D'une part, cette adresse peut contenir des éléments utiles pour retrouver l'identité de son titulaire. D'autre part, il existe des services spécialisés visant à identifier le titulaire d'une adresse électronique déterminée.

L'utilisateur d'Internet laisse de nombreuses traces sur son passage. Le fonctionnement d'Internet est basé sur le protocole TCP/IP. L'acheminement des paquets de données s'accompagne de renseignements techniques enregistrés, même l'espace d'un instant, dans chaque ordinateur qui a participé au transfert du paquet, en particulier les adresses IP de l'émetteur et du destinataire. Certes, l'adresse IP, qui se présente comme une suite de chiffres, ne permet pas d'identifier directement une personne physique déterminée mais une machine particulière dont se servent un ou parfois plusieurs individus. S'il est vrai que l'adresse IP peut être attribuée de manière relativement aléatoire par les fournisseurs d'accès à Internet (surtout dans le cas de petits utilisateurs), il n'en reste pas moins que ces fournisseurs savent à quel utilisateur correspond une adresse IP et peuvent éventuellement opérer des recoupements sur cette base (types de services auxquels l'utilisateur a accédé, etc.). Le problème est encore plus aigu lorsque le fournisseur d'accès à Internet est lui-même fournisseur de services sur Internet. Il peut dans ce cas suivre toutes les opérations réalisées par l'utilisateur au sein de son site.

De la même manière, par le seul accès à un site particulier, l'utilisateur livre de l'information relative à la façon dont il consulte celui-ci [472]. Le serveur Internet peut disposer par là d'un outil permettant d'évaluer le comportement d'un individu. En termes de marketing, savoir à quel moment les yeux d'un lecteur s'arrêtent dans la lecture d'un catalogue publicitaire ou quelles en sont les pages les plus fréquemment consultées est loin d'être anodin.

Les données sont quelquefois obtenues par des moyens manifestement déloyaux. Ainsi, au Québec, on a remarqué que l'accès à certains serveurs s'adressant plus particulièrement aux enfants pouvait être conditionné par le fait de compléter un questionnaire relatif à leurs habitudes de vie ou à celles de leurs frères et soeurs ou de leurs parents. En Belgique,

---

472 Il ne s'agit pas réellement d'une caractéristique propre à Internet mais plutôt à l'utilisation de services interactifs.

l'agence Belga s'est récemment fait l'écho de l'accès non autorisé d'un *surfer* à des données bancaires [473]. Bien que l'information ait été minimisée par la suite, il n'en reste pas moins qu'il s'agit d'un réel danger. En témoignent les affaires de vols de fichiers (par exemple le fichier clientèle) donnant lieu à des chantages et relatées par la presse spécialisée [474].

Récemment, le phénomène des *cookies* est apparu sur le réseau. Cette technique permet à un serveur « d'imprimer » sur chaque navigateur des informations qu'il détermine. Bien que le contenu de ces *cookies* ne réponde à aucune norme, le serveur y inscrira généralement l'adresse de la dernière page *web* consultée ainsi que la date d'expiration du *cookie*. Ce mécanisme permet ainsi à un serveur Internet de « reconnaître » un utilisateur qui a interrogé son site précédemment. Mais il est également possible pour un serveur Internet de connaître de cette manière les dernières pages *web* visitées par l'utilisateur en question. L'impact du *cookie* peut être plus pernicieux encore et conduire à une véritable collecte de l'information présente sur l'ordinateur de l'utilisateur.

Finalement, il semble que les nouveaux programmes de navigation puissent transmettre aux sites interrogés de nombreuses informations sur le profil de l'utilisateur. Cette possibilité pourrait être amplifiée par l'utilisation de *scripts* JAVA, petits programmes transmis par le serveur Internet auquel l'utilisateur est connecté et exécutés à son insu, sur sa machine, par le programme de navigation. Bien souvent, ces *scripts* JAVA n'exécutent que des actions anodines (par exemple l'animation d'un logo à l'écran), mais il est techniquement possible que ces *scripts* en exécutent d'autres qui le sont nettement moins...

On le voit, les enjeux posés par Internet en termes de protection des données à caractère personnel sont de taille. De par le nombre d'informations disponible à partir du réseau, Internet constitue une source importante d'informations. L'utilisation d'Internet génère de nombreuses données à caractère personnel et les caractéristiques propres de ce réseau en favorisent la dissémination.

Le risque d'atteinte aux droits et libertés fondamentaux s'exprime de manière générale par la perte de contrôle de l'individu sur les données qui le concernent et sur les utilisations qui peuvent en être faites. En effet, le fonctionnement du réseau Internet se caractérise par une grande opacité en termes de collecte et d'enregistrement des données. L'individu ne sait généralement pas quelles données sont collectées, par qui, auprès de qui, dans quel but.

---

473 Voir les dépêches Belga des 27 et 28 janvier 1997 mettant en cause Belgium OnLine et le Crédit Professionnel. Ce dernier avait lancé un compte spécial permettant aux utilisateurs d'Internet d'effectuer gratuitement et « en toute sécurité » des opérations et des paiements bancaires.

474 Voir, à titre d'exemple, « Chantage informatique sur l'Internet », *Expertises*, 1996, p. 336.

Le cas est particulièrement évident en cas de mise à disposition de données sur un serveur Internet. En effet, d'une part, l'identification de la personne qui gère le serveur peut s'avérer difficile. D'autre part, les destinataires potentiels de l'information mise à disposition de la sorte sont *a priori* inconnus.

Internet simplifie, en outre, les moyens déloyaux de collecte de l'information auprès de tiers à l'insu des personnes concernées.

Ce réseau facilite également la réutilisation de données pour d'autres buts que ceux pour lesquels l'information avait été communiquée. Ainsi, certains sites permettent de repérer des adresses électroniques qui peuvent être réutilisées par la suite pour l'envoi de messages publicitaires dans les boîtes aux lettres électroniques.

Au surplus, l'individu perd rapidement tout moyen d'entrer en relation avec ceux qui utilisent ses données. Ainsi, si une information erronée est diffusée sur le réseau, il ne sera généralement pas en mesure de retrouver les différents destinataires pour la faire rectifier.

Il existe aussi un risque d'établissement de profils d'individus sur base de la recherche systématique d'informations à travers le réseau. Ainsi, savoir que M. X. a écrit un article dénonçant les mouvements racistes, qu'il participe à un forum de discussions spécialisé dans les questions intéressant les homosexuels et qu'il a envoyé des courriers électroniques à tel et tel destinataires peut s'avérer particulièrement intéressant pour dresser un profil de sa personnalité.

Deux risques méritent encore d'être mentionnés : la dimension internationale du réseau qui amplifie largement les problèmes et peut rendre la mise en oeuvre de législation de protection des données bien aléatoire (voir *infra*) et le risque lié au manque de sécurité apportée aux données. A titre d'exemple, l'émetteur d'un message n'est jamais tout à fait certain de l'identité de la personne à qui il envoie des informations.

Faut-il enfin mentionner l'absence de garantie de qualité des informations glanées ici et là sur le réseau ?

## II. Pistes de Solutions

Face à ce genre de risques, divers types de solutions sont envisageables. Les premières, issues du développement du réseau, peuvent être qualifiées de techniques ou plus largement d'auto-réglementaires. Ainsi, des solutions ad hoc voire des règles de conduite s'élaborent, tendant à rendre harmonieux les rapports entre les différents utilisateurs. Il convient de rappeler à cet égard que l'auto-réglementation est une des caractéristiques intégrantes d'Internet[475].

Certains serveurs indiquent quelles sont les informations qu'ils détiennent au sujet d'un utilisateur. Sur base de l'interrogation de la fonction prévue à cet effet, ils émettent une hypothèse quant à l'identité de l'utilisateur, à la localisation du fournisseur d'accès, au type de machine de l'utilisateur ou au fait d'avoir visité le site récemment...

Les serveurs d'anonymisation offrent aux utilisateurs la possibilité de « se balader » relativement incognito sur le N*et*. Ils fonctionnent globalement de la manière suivante : lors de l'envoi d'un premier message, le serveur d'anonymisation supprime les données permettant d'identifier l'utilisateur, attribue à celui-ci un nouveau « nom » et se charge, par la suite, de lui réexpédier les messages qui lui sont destiné[476].

Il existe sur Internet de nombreux logiciels de cryptage (dont *Pretty Good Privacy* ou *PGP*) qui permettent d'assurer dans une large mesure la confidentialité des données transmises et d'attribuer de manière assez sûre un message à un destinataire déterminé[477].

On peut mentionner bien d'autres exemples de solutions techniques, comme l'introduction du consentement de l'utilisateur à l'installation de *cookies* dans la dernière version du logiciel de navigation Netscape[478].

---

475 Le W*orld Wibe Web* est le résultat de recherches menées dans des centres distincts (ministère de la Défense américaine, M. I. T. et C. E. R. N. ) qui ont conduit à l'élaboration de normes et de procédures communes. D'autres organismes souhaitant exercer un certain contrôle sur le développement d'Internet sont venus s'ajouter par la suite (Internet Society, etc.).

476 Dans la mesure où le serveur d'anonymisation est en mesure d'identifier l'utilisateur, certains estiment qu'il est préférable de passer par plusieurs de ces serveurs.

477 Certaines législations nationales sont très restrictives à l'égard des procédés de cryptage. En Belgique, l'article 95, 5° de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques donne compétence au ministre ayant les Télécommunications dans ses attributions, sur proposition de l'Institut belge des services postaux et des télécommunications, de retirer l'agrément ou d'imposer une interdiction de maintenir le raccordement à l'infrastructure publique de télécommunication d'un appareil terminal qui rendrait inefficace les moyens permettant de réaliser, dans les conditions prévues par le code d'instruction criminelle, le repérage, les écoutes, la prise de connaissance et l'enregistrement des télécommunications privées. On connaît les remous suscités par le « Clipper chip » aux Etats-Unis.

478 Il s'agit de la version Netscape 3. Cette possibilité n'existait pas dans la deuxième version de Netscape.

Ces solutions posent de manière plus large la question de l'intérêt d'une approche fondée sur l'auto-réglementation. Certains avantages d'une telle approche méritent d'être soulignés.

Tout d'abord, l'approche auto-réglementaire fournit des solutions dépassant les frontières nationales et européennes.

De plus, ce type de norme est en principe élaboré au niveau le plus adéquat, c'est-à-dire celui où surgissent les problèmes (serveurs Internet, fournisseurs d'accès, agissant de manière individuelle ou collective...), ce qui contribue tant à la conscientisation des ficheurs qu'à l'effectivité de la mise en oeuvre de celles-ci. De cette manière, des procédures spécifiques apportant des réponses appropriées aux questions qui se posent, peuvent être mises au point.

Finalement, dans la mesure où les règles sont facilement modifiables, elles sont aptes à évoluer parallèlement aux progrès technologiques.

Cependant, les mécanismes d'auto-réglementation présentent des inconvénients majeurs.

Avant tout, il n'est pas certain que le niveau de protection qu'ils sont susceptibles de proposer puisse être qualifié d' « adéquat » selon les termes de la directive européenne, et suffire pour permettre les transferts à destination de pays tiers à l'Union européenne (v. *infra*).

Ensuite, dans la mesure où ils sont fondés essentiellement sur le volontariat de ceux qui sont amenés à les adopter et à les mettre en oeuvre, le caractère effectif de la protection qu'ils sont à même d'apporter peut être sérieusement mis en cause.

Enfin, ils ne sont pas soumis à une publicité organisée et ne tiennent compte que dans une certaine mesure de l'intérêt des individus. En effet, même si leurs rédacteurs sont souvent conscients de la nécessité d'assurer une protection des personnes concernées par les données, ils la traduisent dans leur propre logique, généralement sans qu'un réel débat réunissant tous les intéressés n'ait eu lieu.

Les tentatives de solutions issues de l'auto-réglementation ne sont donc adéquates que jusqu'à un certain point. Une autre voie de solution peut être également envisagée : celle faisant intervenir l'action législative.

Le recours à l'instrument législatif a le mérite de rencontrer deux préoccupations qui n'étaient qu'imparfaitement prises en compte par les autres voies de solution. A l'incertitude de l'auto-réglementation, la loi oppose la sécurité juridique puisque, par nature, elle s'accompagne de force juridique contraignante, qui est la meilleure garantie de l'efficacité des principes adoptés. Par ailleurs, si l'auto-réglementation, par son caractère trop souvent unilatéral et par les choix techniques *a priori* qu'elle pose, présente le défaut de ne pas véritablement opérer une balance des intérêts contradictoires en présence, le processus législatif, quant à lui,

offre l'avantage d'impliquer dans son déroulement une mise en balance des forces et intérêts contradictoires. La loi est l'expression du résultat atteint.

L'action législative a donc sa raison d'être, mais est-elle pour autant pertinente ? L'exemple de législation qui s'impose pour évoquer cette question est celui de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Dans le domaine de la protection de la vie privée face au traitement des données à caractère personnel, c'est à ce jour l'exemple par excellence car, non seulement c'est le texte le plus représentatif sur la scène européenne, mais, dernière-née dans le panorama législatif européen, la directive est également censée être le texte le plus avancé en la matière au regard des nouvelles perspectives technologiques.

Il reste à s'interroger : la directive est-elle un instrument opportun ? Apporte-t-elle les réponses adéquates face au phénomène d'Internet ?

# III. La réponse de la directive européenne relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[479]

## III.1. Portée de la directive

La directive vise à protéger les libertés et droits fondamentaux des individus, notamment leur vie privée, par le biais de la protection des données à caractère personnel, afin d'assurer en contrepartie la liberté des flux d'information sur tout le territoire communautaire[480].

### *III.1.1. Les données à caractère personnel*

Les données bénéficiant de la protection mise en place sont celles qui se rapportent à une personne physique, un individu identifié ou identifiable sans trop grande difficulté[481]. Pour être couverte par la directive, l'information ne doit pas nécessairement concerner la « vie privée » entendue dans son sens classique, c'est-à-dire qu'elle ne doit pas obligatoirement se rapporter à ces éléments de la vie des individus que ceux-ci souhaitent soustraire au regard du public, qu'il s'agisse notamment de leur état de santé, de leurs convictions religieuses, de leur vie familiale, etc. Toute information, quel que soit son contenu, est considérée comme « à caractère personnel » dès lors qu'elle peut être rattachée à un individu déterminé.

Ainsi les adresses électroniques personnalisées (contenant des éléments suffisants pour établir l'identité de leurs titulaires - nom, prénom ou initiales par exemple) entrent dans le champ de la directive. Il en est de même des adresses non « parlantes » mais dont on connaît le titulaire. Les données de routage, l'empreinte électronique laissée lors de l'utilisation de services présents sur le *Net*[482], ne sont pas porteuses d'identification *a priori* mais si les moyens d'identification, c'est-à-dire de rattachement

---

479 Pour une analyse détaillée de la directive, v. également C. de TERWANGNE et S. LOUVEAUX, « Data protection and on-line networks », à paraître dans *Computer Law & Security Report.*

480 Cf. l'intitulé très explicite de la directive ainsi que l'art. 1er §§ 1 et 2.

481 Art. 2. a. V. également le considérant 26 « ... pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne ».

482 V. *supra.*

entre une donnée et l'identité d'un individu, sont à la portée du détenteur de la donnée, celle-ci doit être considérée comme à caractère personnel. C'est notamment le cas s'il a été demandé à l'interrogateur de s'identifier une première fois, au départ de ses opérations dans un site donné. Ce l'est aussi pour le fournisseur d'accès puisque c'est lui qui a attribué une adresse IP (la donnée de routage) à l'utilisateur. De même, si un lien contractuel ou autre existe entre le fournisseur d'information et celui qui détient la clef d'identification, les données peuvent être considérées comme couvertes par la directive dans le chef du fournisseur d'information.

La forme que prennent les données importe peu. Si l'on pense traditionnellement aux données écrites (quel que soit leur support - papier, électronique ou autre), il convient de prendre également en considération les sons et les images. Pour autant que ces derniers véhiculent des informations à caractère personnel, ils sont en effet expressément visés par les auteurs de la directive[483]. L'univers d'Internet sous toutes ses formes est donc susceptible de tomber dans le champ de la directive.

### *III.1.2. Le traitement*

Les individus sont protégés à l'égard du traitement des données les concernant. Il faut donc que des opérations soient effectuées sur les données pour que la directive trouve à s'appliquer. La notion de « traitement » retenue dans le texte communautaire est toutefois à ce point large que toute opération, depuis la collecte jusqu'à la destruction en passant par l'extraction, la consultation ou la communication - notamment - est constitutive de traitement[484].

Une question particulière concerne la consultation proprement dite. Chacune des opérations citées dans la définition du traitement, même prise isolément, met en présence d'un traitement. En conséquence, la simple consultation d'informations à caractère personnel devrait impliquer l'existence d'un traitement. Or, la vocation première d'un système tel qu'Internet est de permettre la circulation et la consultation d'informations. Il est clair que dans ce contexte, la définition adoptée dans la directive conduit à une multiplication exponentielle des traitements effectués. Traitements qui, dans le cas de simples consultations, ne sont pas sans susciter de sérieuses interrogations. Ainsi, faut-il informer les personnes concernées dès que l'on consulte un site contenant des données à leur sujet et même si l'on n'a retenu aucun élément intéressant ou pertinent suite à cette

---

483 V. considérants 14 : « compte tenu de l'importance du développement en cours, dans le cadre de la société de l'information, des techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer les données constituées par des sons et des images, relatives aux personnes physiques, la présente directive est appelée à s'appliquer aux traitements portant sur ces données » et 15.

484 V. art. 2. b.

consultation ? En outre, si la consultation des données n'est suivie d'aucune matérialisation - les données consultées ne sont ni copiées, ni enregistrées, ni imprimées - que faut-il notifier à l'autorité de contrôle puisque l'éphémère opération n'a laissé aucune trace ? Et comment accorder aux personnes concernées un droit d'accès à une information qui est tout au plus conservée dans la mémoire humaine ? Il y a donc un problème logique à considérer la seule consultation comme constitutive de traitement.

Par ailleurs, l'énumération reprise dans la définition de l'article 2. b est sous-tendue par une chronologie des opérations retenues. Elle débute par la collecte des données et s'achève par la destruction de celles-ci. Or la consultation n'est pas citée en début de liste, précédant l'opération de collecte. Elle apparaît au contraire entre l'extraction et l'utilisation, la communication... Il semble donc que ce qui est visé dans la directive ce n'est pas la consultation dans le chef de celui qui fait une « lecture » des données, mais plutôt la possibilité d'opération offerte par le traitement, le fait de laisser consulter les données. C'est d'une « offre en consultation » qu'il s'agit plutôt.

La définition du traitement donnée par la directive est suffisamment large pour intervenir, et donc pour permettre à la protection de la directive de jouer, dès que des données sont collectées ou enregistrées. Dans ces deux hypothèses, à l'inverse de la consultation, le traitement a une matérialité. Il n'y a donc pas de nécessité d'englober des situations dans lesquelles seule une prise de connaissance est observée. Dès que cette prise de connaissance donnera lieu à un copiage, un encodage ou toute autre forme de collecte ou d'enregistrement, la directive lui sera appliquée.

La consultation peut donc être retenue comme partie d'un traitement (les données collectées, enregistrées, classées, voire modifiées sont ouvertes à la consultation, par exemple) mais on ne doit pas considérer comme constitutive d'un traitement la seule « lecture » qui n'a aucune prolongation matérielle.

## III.2. Applicabilité de la directive

Avant de centrer l'analyse sur certains points de portée matérielle, les premiers éclaircissements à apporter concernent le champ d'action du texte européen. Quelles activités développées dans le cadre du réseau mondial tombent sous le coup de la directive et doivent désormais[485] respecter les dispcsitions qui y sont contenues[486] ?

---

485 L'article 32 de la directive prévoit que les Etats membres mettent en vigueur les dispositions nécessaires pour se conformer au texte au plus tard à l'issue d'une période de 3 ans (à compter du 24 octobre 1995).

Les critères de rattachement traditionnels pour déterminer l'applicabilité d'une loi consistent en la nationalité des acteurs ou le territoire sur lequel se déroule l'action. Or de tels critères n'ont plus de pertinence dans le cybermonde. La réalité est transnationale, elle court le long des fils de la toile, elle circule sans domicile fixe.

Les auteurs de la directive ont développé une solution intéressante tenant compte jusqu'à un certain point de l'évolution de la technologie. Le texte s'écarte de la notion de « fichier », déterminante dans les premières générations de législations en la matière et basée sur une localisation physique précise des données (sur une disquette, sur le disque dur d'un ordinateur identifié...), pour se centrer sur le traitement qui est effectué sur les données sans que celles-ci soient nécessairement extraites *a priori* et rassemblées en un lieu unique. La géographie n'étant plus d'aucun secours dans cette situation, c'est la notion de responsable du traitement qui est retenue pour définir la loi applicable. Le responsable du traitement, lui, doit nécessairement être établi sur un territoire. Si ce territoire est partie de l'Union européenne, c'est la loi nationale de l'Etat concerné transposant les préceptes de la directive qui s'appliquera aux traitements effectués par le responsable dans le cadre de ses activités (art. 4. 1. a). Ainsi, si une entreprise danoise ouvre un site sur Internet présentant notamment ses cadres avec une brève identification, elle doit respecter la loi danoise de protection des données. Si un complexe hôtelier espagnol offrant un service de réservation via Internet demande aux intéressés d'enregistrer leurs coordonnées afin d'effectuer la réservation, la loi espagnole de protection des données s'appliquera au traitement de ces informations (qu'elles concernent des Français, des Russes, des Américains ou des Japonais).

En résumé, donc, tous les responsables de traitement établis au sein de la Communauté européenne sont tenus de respecter la directive lorsqu'ils traitent des informations à caractère personnel.

Les responsables situés en-dehors du territoire communautaire ne sont pas concernés par la directive. Toutefois, le législateur européen s'est préoccupé des tentatives de contournement des prescriptions communautaires par la délocalisation de l'établissement du responsable du traitement. Afin d'éviter pareille situation, le texte prévoit que tout responsable établi à l'extérieur de l'Union mais qui recourt à des moyens, automatisés ou non, situés sur le territoire d'un Etat membre, dans le but de traiter des informations nominatives, doit se soumettre à la législation de protection des données de cet Etat. Il doit en outre désigner un représentant établi dans le pays en question (article 4.1.c).

Dans le contexte d'Internet, une telle solution est impraticable à première lecture. Elle conduit *a priori* à étendre l'application de la direc-

---

486 Telles bien sûr que transposées dans les différents droits nationaux.

tive à tout utilisateur d'Internet venant à copier des données à caractère personnel à partir d'une base de données ou d'un site *web* produits par un acteur situé sur le territoire communautaire.

En effet, d'après la directive c'est bien lorsqu'on utilise, pour effectuer un traitement de données, *des moyens localisés dans un Etat membre*, que le traitement en question est soumis à la loi de cet Etat membre. S'il est clair qu'il y a recours à des moyens localisés dans un Etat membre quand il s'agit de lancer un questionnaire dans un Etat afin d'obtenir des informations nominatives sur les habitudes de consommation ou quand on interroge la base de données reprenant le registre central de commerce d'un pays afin de connaître les coordonnées des membres d'un secteur d'activités, il est beaucoup moins aisé de « localiser » les moyens utilisés dans les hypothèses de recours à Internet.

Internet constitue un espace où l'information est a-localisée même si les personnes et les sites s'identifient par des « adresses ». Ces adresses sont en fait des clefs, les serrures et ce qu'elles cachent n'étant pas nécessairement géographiquement stables. Lorsque l'adresse aboutit sur un réseau interne, le site peut être « logé » sur n'importe quel ordinateur relié à ce réseau. Dans le cas d'un réseau interne à une entreprise, par exemple, l'adresse du site peut correspondre à un ordinateur placé dans le bureau du directeur ou de la documentaliste. Si le réseau interne relie un ensemble de postes dispersés de par le monde, l'adresse électronique pourrait, restant la même, aboutir à un poste situé à Anvers ou à Singapour.

Pour trouver le correspondant géographique d'un site Internet deux solutions sont envisageables :

— Soit remonter à la localisation de la machine, de l'ordinateur qui assure le maintien de l'information sur le site en question. Il est cependant possible de confier à un intermédiaire la mission d'héberger l'information que l'on souhaite mettre à disposition sur Internet. Dans cette hypothèse, l'adresse électronique correspond à une boîte postale ouverte pour la circonstance mais ne révèle pas de lien direct avec la source de l'information.

— Soit on peut identifier le responsable de l'information, celui qui l'a produite, et on retient le lieu de son établissement. Ainsi si une université fournit sur son site *web* une base de données bibliographiques des oeuvres de ses membres, on considérera que ce site sera géographiquement localisé au lieu d'établissement de l'université en question. Cette solution offre l'avantage de la cohérence avec le critère de rattachement adopté par la directive concernant les traitements effectués par un responsable établi sur le territoire communautaire.

Il faut relever qu'il n'est pas toujours évident de connaître le lieu d'établissement du fournisseur d'information. Or c'est ce lieu qui détermine la loi nationale à respecter et qui désigne le pays dans lequel le res-

ponsable de traitement étranger devra nommer un représentant. Comment savoir à quels pays correspondent des adresses - tirées de la réalité - telles que '105473.8880@compuserve.com' ou 'http://www.telepathic.com' ? Et comment un Taïwannais pourra-t-il savoir si la ville de Gävle qui fournit une liste exhaustive des pêcheurs de morue de la Baltique est située en Suède ou en Estonie (et de surcroît, dans ce dernier cas, hors Communauté) ?

Par ailleurs, la situation particulière des forums et autres « lieux » de rencontre ou d'échange soulève une difficulté supplémentaire. Pour les localiser, recourt-on à l'établissement du modérateur ou « maître du forum » ?

Une fois les « moyens » localisés en territoire européen, on sait que la directive s'applique dès que ces moyens sont utilisés pour effectuer un traitement. Or la définition du traitement contenue à l'article 2. b. de la directive est très large et recouvre un éventail complet d'activités, chaque activité prise isolément pouvant constituer un traitement [487]. Ainsi, copier des données revient à les collecter, ce qui est en soi constitutif de traitement aux yeux de la directive.

En conséquence, celui qui par la voie d'Internet, télédécharge des données nominatives à partir d'un site ouvert par un fournisseur d'information établi dans un Etat membre, effectue par là-même un traitement pour lequel il a recouru à des moyens (automatisés *in casu*) rattachés au territoire communautaire. Dans cette situation, il est tenu de respecter la réglementation européenne et de désigner un représentant établi dans l'Etat concerné.

C'est évidemment excessif.

Pour garder à l'article 4.1.c. une portée effective, la seule lecture de cette disposition qui semble, à notre sens, devoir s'imposer est une lecture téléologique. La *ratio legis* de cet article se résume clairement dans la volonté d'éviter que les individus se trouvent dépourvus de toute protection, en particulier du fait d'un contournement de la législation[488]. Le souci des auteurs du texte est donc d'assurer une protection à ceux qui doivent

---

487 Par traitement il faut entendre « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

488 Cf. le considérant 20 de la directive, 1ère phrase : « considérant que l'établissement, dans un pays tiers, du responsable du traitement des données ne doit pas faire obstacle à la protection des personnes prévue par la présente directive; ... » et l'exposé des motifs : « (L'article 4) fixe les critères de rattachement permettant de déterminer quelle est la législation nationale applicable aux traitements entrant dans le champ d'application de la directive et ceci afin d'éviter (...) que la personne concernée soit démunie de toute protection, en particulier du fait d'un contournement de législation » (Proposition modifiée de Directive du Conseil, 15 octobre 1992, COM(92) 422 final - SYN 287, p. 13).

normalement en bénéficier sous l'égide de la directive, même en-dehors des frontières communautaires.

C'est par une lecture combinée de l'article 4.1.c et des articles 25 et 26 qui régissent les flux transfrontières vers les Etats tiers qu'une définition rationnelle de l'applicabilité de la directive pourra être dégagée.

On peut, en effet, considérer qu'une première réponse à la préoccupation des auteurs de la directive est donnée par l'instauration d'un régime protecteur en matière de flux transfrontières de données vers les pays tiers à la Communauté (cfr. *infra*). Dans le cadre de la réglementation de ces flux, les exigences édictées par la loi européenne s'imposent à tous les acteurs qui effectuent des opérations sur des données fournies à partir de l'Europe. Une protection adéquate des données envoyées à l'étranger en provenance de l'Union est exigée.

La réponse contenue dans l'article 4.1.c vise à couvrir, quant à elle, les situations dans lesquelles les sujets des données se voient privés, par une manoeuvre artificielle, du bénéfice de la protection de l'ensemble de la directive, et les situations échappant à toute protection, même celle instaurée en matière de flux transfrontières. Dans ce sens, deux catégories de situations entrent, selon nous, dans le champ de l'article 4.1.c :

— celle précisément où un responsable de traitement cherche délibérément à contourner la directive et, pour ce faire, délocalise son établissement vers un pays tiers, tout en faisant usage de moyens localisés sur le territoire communautaire pour réaliser son traitement.

— celle où le flux est le fait exclusif d'un responsable localisé dans un pays tiers. C'est le cas d'une collecte de données effectuée par le biais de *cookies*, à l'insu de la personne concernée, au sein même de son poste de travail. Les articles 25 et 26 ne trouvent pas à s'appliquer dans cette hypothèse car les règles protectrices relatives aux flux transfrontières ne s'adressent qu'à l'émetteur d'un flux, et pour autant bien sûr que celui-ci se situe en territoire européen. Or, on ne peut voir dans la personne « visitée » par les *cookies* un véritable émetteur des données prélevées puisque l'opération se déroule à son insu. Pour combler le vide de protection, l'article 4.1.c a alors toute sa pertinence. C'est donc le régime complet de la directive qui va s'appliquer au traitement de données obtenues à l'aide de *cookies*, et non le régime spécifique — plus souple — des flux transfrontières.

Dans ces deux hypothèses, le critère déterminant de l'application de la directive aux responsables établis hors de la Communauté ne se réduit pas à l'utilisation de moyens situés sur le territoire d'un Etat membre. Cette utilisation n'est qu'un élément de l'analyse du contexte des opérations effectuées. Une analyse plus globale s'impose en effet pour pouvoir constater le cas échéant que le responsable du traitement est anormalement établi à l'étranger alors que son activité est orientée sur l'Europe, ou que

l'on se trouve en présence d'une situation échappant à toute protection, notamment à celle issue du régime des flux transfrontières.

## III.3. Régime de protection instauré par la directive

### *III.3.1. Les principes de base de la protection*

Le régime de protection instauré par la directive tient essentiellement à deux principes : le principe de transparence et le principe de finalité.

#### III.3.1.1. Le principe de transparence

Le principe de transparence repose sur l'instauration de la connaissance comme clef de la maîtrise. Le but d'un régime de protection des données à caractère personnel est de permettre à chaque individu de savoir qui sait quoi sur lui et pour en faire quoi. C'est à cette seule condition de connaissance que peut s'exercer la maîtrise par chacun du sort réservé aux informations qui le concernent, à son « image informationnelle ».

La maîtrise elle-même prend différentes formes. Elle peut s'exprimer par le consentement donné, refusé ou négocié à la divulgation, à l'utilisation ou à la transmission des informations. Elle se situe également dans le contrôle de la qualité des données et le pouvoir corrélatif d'imposer des corrections. Et c'est encore de maîtrise qu'il s'agit lorsque le sujet se voit reconnaître des recours en cas d'usage illégitime des données, et ce notamment dans les situations qui échappent au départ à son consentement (lorsque le traitement est, à la base, directement justifié par une loi, par exemple, ou par l'intérêt prédominant d'un tiers, mais qu'il y a utilisation abusive des données).

Les deux instruments majeurs de la transparence sont le devoir d'information des personnes fichées, qui pèse dans le chef du responsable de traitement, et le droit d'accès des personnes concernées aux données enregistrées à leur propos.

Lorsqu'il collecte des données, que ce soit directement auprès des personnes concernées ou indirectement, par le biais d'un intermédiaire ou par l'achat d'un fichier, par exemple, le responsable du traitement doit communiquer aux individus fichés son identité et la ou les finalités liées qu'il poursuit en effectuant le traitement des données. Le cas échéant, il

doit également préciser les destinataires ou catégories de destinataires des données[489].

Le droit d'accès répond au même objectif de transparence à l'égard des personnes concernées mais se situe du point de vue de ces dernières. Chacun a le droit non seulement de savoir si des informations à son sujet sont traitées par un responsable de traitement visé, mais également d'obtenir une copie - sous forme compréhensible - des données faisant l'objet du traitement. La directive comporte même une disposition originale par rapport à la majorité des législations nationales antérieures : elle reconnaît aux personnes concernées le droit de connaître l'origine des données enregistrées[490].

#### III.3.1.2. Le principe de finalité

Le principe de finalité conduit à exiger que tout traitement ait une ou des finalités précises et légitimes. C'est dès avant la mise en œuvre d'un traitement que la finalité doit être déterminée[491]. La légitimité de la finalité est laissée à l'appréciation des parties, sous bénéfice de contrôle par le juge voire par une autorité de contrôle ad hoc.

Outre l'exigence de légitimité, le principe de finalité implique également que toute utilisation des données soit compatible avec la finalité annoncée lors de la collecte des données[492]. La directive ne précise pas ce qu'il faut entendre par « utilisation compatible » mais on peut, selon nous, comprendre ces termes dans le sens d'une « utilisation correspondant à l'attente raisonnable des personnes concernées » au vu de la finalité première annoncée. Dans le cas où un auteur publie des articles par le biais d'un site Internet offrant cette possibilité, il peut raisonnablement s'attendre à ce que le gestionnaire du site utilise ses coordonnées pour le tenir au courant des manifestations (colloques, conférences, rencontres) organisées sur le thème traité, ou pour les transmettre à des éditeurs scientifiques. Celui qui recourt à des services bancaires peut raisonnablement s'attendre à ce que l'organisme bancaire utilise ses données personnelles pour le faire bénéficier d'opérations de marketing concernant les produits ou services financiers offerts par la banque en question. L'utilisateur d'Internet qui s'adresse à un fournisseur d'accès pour pénétrer dans le réseau peut s'attendre à ce que le fournisseur d'accès utilise les données se rapportant à ses interrogations pour lui proposer des conditions spéciales

---

489 V. pour le détail les articles 10 et 11 de la directive.

490 Art. 12. a.

491 Puisqu'une notification reprenant notamment la ou les finalités du traitement doit être adressée à l'autorité de contrôle « préalablement à la mise en œuvre d'un traitement entièrement ou partiellement automatisé ou d'un ensemble de tels traitements ayant une finalité ou des finalités liées » (art. 18 et 19).

492 Art. 6. 1. b

d'abonnement tenant compte, par exemple, de la fréquence des appels. Ces utilisations secondaires doivent donc être considérées comme compatibles avec les finalités initiales des traitements. Entrent également dans la notion d'attente raisonnable les opérations effectuées sur les données en application de textes de loi (lois pénales ou fiscales, par exemple). L'individu qui ouvre un compte en banque doit s'attendre à ce que les données relatives à ce compte soient communiquées aux autorités compétentes si une enquête à son égard est menée pour cause de suspicion de participation à des opérations de blanchiment d'argent.

Si les opérations effectuées ne sont pas compatible avec l'objectif initial, il faut considérer qu'on se trouve dès lors en présence d'un nouveau traitement de données pour lequel il est nécessaire d'informer les personnes concernées. La nouvelle finalité doit, à son tour, être légitime. Ainsi, les coordonnées des abonnés téléphoniques sont reprises dans les annuaires dans le but de permettre l'identification du numéro d'appel d'un correspondant recherché. La vente de ces coordonnées par l'organisme de télécommunications à des sociétés privées à des fins de (télé)marketing correspond à un traitement différencié car il s'agit d'une utilisation incompatible avec la finalité première. Elle doit donc être notifiée aux abonnés.

#### III.3.1.3. Le contexte d'Internet

Que deviennent ces principes dans le contexte d'Internet ?

La maîtrise par chacun des informations qui le concernent et du sort qui leur est réservé risque fort, il faut le reconnaître, d'être plus virtuelle que réelle. Vu le nombre d'acteurs qui interviennent dans un réseau ouvert de cette dimension et les possibilités de réutilisations des données disponibles, comment réellement contrôler qui détient l'information et dans quel but elle est utilisée ? Comment connaître l'identité de tous ceux qui télédéchargent les données à caractère personnel présentes sur les sites ? Et surtout, comment vérifier que les traitements effectués pas ces personnes sont compatibles avec les finalités de départ ou que leurs finalités nouvelles sont légitimes ?

Par ailleurs, on constate en contrepartie que, par ses possibilités techniques, Internet permet d'informer les personnes concernées à bien moindre coût et bien plus rapidement que dans un environnement plus classique. En effet, à partir du moment où l'on dispose des adresses électroniques des personnes à contacter, il suffit d'envoyer un message par ce biais et l'objectif est atteint. D'autre part, la présentation des sites peut être configurée de telle sorte que l'information relative au responsable du traitement et aux finalités poursuivies apparaisse d'entrée de jeu sur l'écran. En outre, les possibilités d'interactivité donnent au consentement des personnes concernées une portée nouvelle, dans la mesure où ces dernières

peuvent moduler leur consentement à voir leurs données enregistrées et traitées, en fonction des opérations qu'elles veulent effectuer sur le site visité ou au fur et à mesure de leurs investigations. Elles peuvent déterminer les utilisations des données qu'elles acceptent, en cochant les cases correspondant aux utilisations consenties ou refusées parmi une liste proposée au départ de la consultation, par exemple. L'interactivité donne aux techniques d'*opting-in* ou d'*opting-out* une dimension immédiate et effective. La notion de consentement elle-même prend une nouvelle signification.

Les moyens sont donc à la disposition des bonnes volontés pour respecter le prescrit communautaire.

Les mauvaises volontés seront bien sûr difficiles à contrôler et à traquer mais il faut constater que, hors du contexte d'Internet, il n'est pas non plus facile pour les individus de suivre le cheminement de leurs données personnelles. La différence majeure que présente la toile mondiale c'est l'ampleur du phénomène. Le relais des solutions techniques a, à ce stade, tout son intérêt. De même le rôle des codes de conduite sectoriels par lesquels les secteurs d'activité s'auto-réglementent, faisant de la protection des données à caractère personnel un instrument de la qualité des services offerts, prend toute son importance.

### *III.3.2. Les flux transfrontières de données*

L'objectif de la directive est officiellement d'instaurer une harmonisation des protections au sein de l'Union européenne pour pouvoir, en conséquence, permettre la liberté des flux de données à caractère personnel. On ne peut, en effet, que constater que l'échange de ces données, considérablement facilité par les progrès des technologies de l'information, est devenu une nécessité pour le développement de tous les domaines de l'activité économique et sociale. Les flux transfrontières des données sont en augmentation sensible et constante, impliquant des acteurs tant publics que privés. Ainsi, « l'échange de données à caractère personnel entre des entreprises établies dans des Etats membres différents est appelé à se développer; les administrations des Etats membres sont appelées, en application du droit communautaire, à collaborer et à échanger entre elles des données à caractère personnel afin de pouvoir accomplir leur mission ou exécuter des tâches pour le compte d'une administration d'un autre Etat membre, dans le cadre de l'espace sans frontières que constitue le marché intérieur »[493].

Il est clair que le phénomène d'Internet fait office de catalyseur en matière de flux transfrontières, démultipliant les possibilités et les réalités

493 Considérant 5 de la directive.

des transferts. La toile ayant vocation à couvrir le monde, c'est bien au-delà des frontières communautaires que les données sont susceptibles d'être envoyées.

**III.3.2.1. Le principe : l'exigence de protection adéquate**

Dans de telles circonstances, la préoccupation première vise à éviter que le système de protection ne soit ruiné dès que les données sortent du territoire de l'Union. La directive a donc mis en place des exigences concernant la protection offerte dans les pays tiers. Le principe est que l'on ne peut exporter des données nominatives vers un Etat qui n'offre pas un niveau de protection adéquat (article 25.1).

Le niveau de protection en question doit être évalué en fonction des risques qui s'attachent à chaque flux. Ainsi, la communication d'une liste de délinquants sexuels à une association offrant des services sociaux ou le transfert de la liste des adhérents d'un parti politique à une société de marketing présentent des risques élevés d'atteinte aux libertés des individus, par le biais de l'utilisation de leurs données. En conséquence, il convient d'évaluer de manière sévère l'adéquation de la protection offerte dans le pays tiers. Par ailleurs, on sera moins exigeant en présence d'un flux de données moins sensibles telles que les nom, fonction et durée d'ancienneté des travailleurs, intervenant entre la filiale et la maison mère d'une société. Au regard des circonstances encadrant pareil flux, étant donné le degré moindre de dangerosité qu'il présente, on admettra plus rapidement qu'un système de protection étranger est satisfaisant.

La notion de protection « adéquate » doit s'entendre dans une optique fonctionnelle, c'est-à-dire que ce qui est recherché c'est un système garantissant la mise en œuvre des principes fondamentaux de la protection des données. Il ne s'agit pas d'une approche textuelle qui conduirait à rechercher une similarité de réglementation. La protection doit être assurée de façon adéquate, quelle que soit la forme qu'elle prend. Si le pays tiers dispose d'une règle générale en matière de secret médical, notamment, cette règle pourra être retenue comme un élément valable de la protection dans la mesure où elle limite les réutilisations, même si initialement elle ne vise pas spécifiquement le traitement des données.

En conclusion, pour mesurer le degré de risque que présente un flux de données particulier, il faut tenir compte de toutes les caractéristiques de ce flux : la nature des données en cause, la finalité et la durée du traitement envisagé, les pays d'origine et de destination finale (article 25.2) mais aussi les liens existant entre les intervenants, le type de réseau (ouvert ou fermé) employé... en réponse à cette évaluation, on procède à une analyse de tous les éléments concourant à assurer une protection aux données, une fois celles-ci transférées. Pour ce faire, il convient de retenir tant les règles

de droit générales ou sectorielles que les règles professionnelles, les clauses contractuelles ou les mesures de sécurité d'application.

#### III.3.2.2. Les exceptions

La directive invite[494] les Etats membres à admettre des exceptions au principe qui vient d'être énoncé et à permettre en certains cas le transfert de données nominatives vers des pays n'offrant pas un niveau de protection adéquat.

C'est le cas notamment lorsque la personne concernée a indubitablement donné son consentement à l'opération de transfert (article 26.1.a). On ne peut parler de véritable consentement que si celui-ci est « éclairé »[495], c'est-à-dire si la personne concernée a conscience qu'il s'agit bien d'un flux transfrontalier, connaît le pays de destination des informations qu'elle transmet et réalise que ce pays n'assure pas un niveau de protection adéquat des données.

Des exceptions valent également si la transmission des données intervient dans le contexte d'un contrat liant la personne concernée et le responsable du traitement ou d'un contrat conclu dans l'intérêt de la personne concernée, ou intervient dans le contexte d'une action en justice (article 26.1.b, c, d).

Des dérogations sont encore autorisées lorsque le responsable du traitement qui souhaite transférer des données vers un pays tiers offre lui-même, pas le biais de clauses contractuelles, par exemple, des garanties qui pallient l'insuffisance du niveau de protection du pays en cause (article 26.2).

#### III.3.2.3. Le contexte d'Internet

Un réseau mondial tel qu'Internet est la scène de différents types de flux transfrontières : flux actifs ou passifs, conscients ou cachés.

---

494 « Par dérogation à l'article 25 *et sous réserve de dispositions contraires de leur droit national régissant des cas particuliers*, les Etats membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat (...) peut être effectué (...) » (article 26. 1). Les Etats membres peuvent donc, par des dispositions régissant des cas particuliers, refuser que l'une ou l'autre exception s'applique à ces cas. On pense dans un premier temps aux situations mettant en jeu des données sensibles, médicales ou judiciaires. Mais la particularité des cas retenue peut être plus large et consister non plus dans le caractère sensible des données mais, par exemple, dans la nature du réseau - ouvert ou fermé - utilisé. On peut donc imaginer qu'un Etat membre soit plus strict qu'un autre en matière d'exceptions appliquées à l'utilisation d'un réseau tel Internet.

495 Cf. la définition du consentement donnée à l'article 2. h de la directive : « toute manifestation de volonté, libre, spécifique *et informée* » et l'Exposé des motifs, Proposition modifiée de Directive du Conseil, 15 octobre 1992, COM(92) 422 final - SYN 287, p. 36 : « Le transfert vers un pays tiers n'assurant pas un niveau de protection adéquat peut être effectué si la personne concernée a donné son consentement au transfert envisagé (...) Dans ce cas, la personne est informée du transfert ou de la possibilité de transfert vers un ou des pays tiers n'assurant pas un niveau de protection adéquat ».

*Les flux actifs conscients* correspondent à des transferts effectués sciemment par le responsable de traitement ou par la personne concernée elle-même. Ces flux peuvent être décidés à l'initiative de l'émetteur ou en réponse à une demande provenant du destinataire. Ils couvrent des hypothèses aussi variées que celles d'un consommateur belge envoyant ses coordonnées à un fournisseur de service canadien, ou d'une banque italienne transmettant des données aux Etats-Unis afin d'effectuer un paiement au nom de son client, ou d'une filiale faisant parvenir son fichier du personnel à la maison mère localisée au Japon, ou encore d'un fournisseur de service français vendant son registre de clients à une société de marketing norvégienne.

De tels transferts tombent souvent dans les catégories d'exceptions de l'article 26 de la directive. Ainsi, les communications de données nominatives effectuées directement par les personnes concernées (comme dans le premier exemple cité) sont indubitablement couvertes par le consentement de ces dernières. Le consentement devant toutefois être « éclairé » pour être valable, la personne concernée doit avoir conscience du pays de destination du flux et du fait que ce pays n'offre pas un niveau de protection adéquat. Or, l'identification de ce pays risque, rappelons-le, de poser un problème dans les cas où la localisation du responsable d'un site n'est pas évidente. Par ailleurs, les flux s'apparentant au deuxième exemple cité tombent dans la catégorie des flux nécessaires à l'exécution d'un contrat entre la personne concernée et le responsable du traitement, tandis que le troisième exemple peut correspondre, au vu des circonstances, à l'exception valable pour les transferts nécessaires à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et un tiers.

Tous les flux actifs conscients ne sont cependant pas couverts par des dérogations. Le dernier exemple cité, notamment, n'entre dans aucune des catégories énoncées dans l'article 26.1. C'est donc la règle de principe qui sera appliquée à l'égard de ces flux et une évaluation devra être faite de la protection offerte dans les pays tiers concernés.

*Les flux actifs cachés* concernent, d'une part, les données de routage, la trace électronique laissée dans le sillage des démarches effectuées dans le réseau mondial et d'autre part, les données discrètement transférées d'un système à un autre par l'action des *cookies*. Ces flux sont actifs, dans la mesure où il y a un réel mouvement des données d'un point à un autre. Ils échappent toutefois à la connaissance des personnes concernées.

Dans ces deux hypothèses, il ne s'agit pas vraiment de transferts de données étant donné qu'une telle opération implique un émetteur et un récepteur. Or, on ne peut parler d'émetteur en présence d'une personne qui n'a pas conscience d'être à l'origine d'un mouvement de données, qui n'a pas manifesté sa volonté d'effectuer ou de voir effectuer le transfert. Plutôt

qu'un flux, c'est une collecte de données qui est réalisée par le « récepteur » lorsqu'il entre en possession des informations.

Le régime des flux n'étant pas d'application, les personnes concernées sont donc démunies de toute protection puisque le responsable du traitement est établi hors du territoire communautaire. Cette situation entre cependant dans le champ de l'article 4.1.c de la directive[496]. En effet, à partir du moment où le responsable du traitement recourt à des moyens localisés sur le territoire d'un Etat membre (collecte au sein du poste de travail de la personne concernée), il doit respecter l'ensemble des dispositions de la directive telles qu'intégrées dans la loi nationale de l'Etat en cause. Dès lors, pour être légitime au regard de la directive, la collecte de données à caractère personnel par le biais de *cookies* doit être loyale et ne peut se faire de façon occulte. Une information appropriée doit être fournie aux personnes concernées et le but poursuivi doit être légitime.

Concernant la trace électronique, le responsable du site étranger visité par une personne située en Europe ne doit pas « recourir à des moyens localisés sur le territoire d'un Etat membre » pour obtenir de telles données. Il lui suffit d'enregistrer les données de routage qui lui sont parvenues suite à l'action du visiteur. Il peut dès lors être plaidé que l'article 4.1.c ne s'applique pas à lui et que, de ce fait, il ne doit pas respecter le prescrit de la directive. Il ne reste plus alors qu'à prévenir les utilisateurs d'Internet que leur action dans le réseau peut ne pas passer inaperçue, même si eux-mêmes ne s'en aperçoivent pas. Ici encore, l'autoréglementation d'un secteur peut apporter une réponse opportune face à la limite de l'instrument législatif, et conduire à la transparence des pratiques. Certains fournisseurs de services ou d'information font de l'information de leurs clients une condition de la qualité et une clef de la confiance.

*Les flux passifs* se rapportent aux informations qui sont simplement mises à la disposition du public sur un site du réseau. Les données sont, en ce cas, potentiellement accessibles de partout et par quiconque. Elles peuvent être télédéchargées et, de ce fait, faire l'objet d'un transfert, vers un pays tiers. Les flux transfrontières sont dits « passifs » dans le sens où ils sont potentiels.

Pour cette catégorie de flux, il importe, avant de déposer de l'information à caractère personnel sur un site, d'évaluer la protection offerte par chaque Etat connecté puisque chacun de ces Etats représente un pays de destination potentiel pour les données. Si un pays se révèle dépourvu de mesures de protection adéquates, l'accès aux données ou, à tout le moins, les possibilités de copiage et de transfert des données doivent être interdits à ces pays.

---

496 Cf. *supra* la lecture téléologique proposée de cette disposition.

On devine la difficulté que représente le respect des dispositions communautaires dans le contexte d'Internet. Difficulté d'autant plus grande quand on pratique le type d'évaluation recommandé par la directive : une évaluation au cas par cas, prenant en considération l'ensemble des circonstances d'un flux donné. Une protection adéquate pour des données telles que le nom, l'adresse et la nationalité d'un individu peut s'avérer ne plus l'être pour la religion pratiquée ou l'état de santé de cette personne. La protection offerte par un Etat tiers peut être jugée satisfaisante pour les secteurs financier et de la recherche, grâce à l'existence de législations ou de codes de conduite spécifiques à ces secteurs, par exemple, mais dans le même temps être considérée comme insuffisante pour les secteurs du marketing ou des loisirs.

## IV. Conclusion

Internet peut apparaître comme le creuset de tous les dangers pour les droits et libertés des individus. Sur la toile mondiale, la maîtrise par chacun du sort des données qui le concernent risque souvent d'être plus virtuelle que réelle. Le phénomène Internet fait cependant l'objet de tentatives de solutions destinées à réduire ces risques. Plusieurs voies peuvent être empruntées. La voie de l'auto-réglementation couplée à celle de la technologie ou la voie législative. Aucune de ces voies n'est en soi complètement satisfaisante. Toutefois, leur combinaison permet de répondre de façon plus adéquate aux problèmes et inquiétudes suscités par les autoroutes de l'information. Elles prennent utilement le relais l'une de l'autre.

Dans ce contexte, la directive européenne, qui n'a pas directement été conçue pour prendre en compte le réseau des réseaux même si ses auteurs en pressentaient l'importance croissante[497], n'en constitue pas moins un instrument législatif dont le mérite est de chercher à exprimer un équilibre entre les droits et libertés des individus et la libre circulation des informations personnelles. Le texte communautaire lui-même encourage l'élaboration et l'adoption de codes de conduite sectoriels, ce qui, aux yeux des auteurs de la directive, permet d'apporter une réponse souple et adaptée à la question de l'application des principes de protection des données aux secteurs concernés. Il reste aux législateurs nationaux chargés de transposer le texte normatif européen, à faire preuve de créativité en activant l'hyperlien adéquat entre cette directive et l'incontournable phénomène contemporain d'Internet.

497 L'article 33 de la directive invite la Commission à réaliser périodiquement une évaluation de l'application de la directive, l'alinéa 2 spécifiant : « la Commission examine, en particulier, l'application de la présente directive aux traitements de données constituées par des sons et des images, relatives aux personnes physiques, et elle présente les propositions appropriées qui pourraient s'avérer nécessaires en tenant compte des développements de la technologie de l'information et à la lumière de l'état des travaux sur la société de l'information. »